付録 1

Asia PKI Interoperability Guideline の

利用に関する手引

－ 目　次 －

1 はじめに

1.1 目的

Asia PKI Forumで策定された「Asia PKI Interoperability Guideline version1.0」（以降「Asia PKI Interoperability Guideline」と記述する)[1]はアジア各国／地域で実施した実証実験の成果に基づいた実績ある仕様であり、安全な電子商取引の基盤確立のために広く利用されるべきものである。本手引きは「Asia PKI Interoperability Guideline」を用いて特恵ECOパイロットシステムのPKI環境を構築した事例を記述したものであり、「Asia PKI Interoperability Guideline」利用の具体例を示し読者の理解を助けることを目的としている。

特恵 ECO パイロットシステムの PKI 環境構築においては、「Asia PKI Interoperability Guideline」のパート II で規定しているアジア諸国・地域において相互運用可能な PKI の枠組みを構築するための推奨技術仕様 （PKI の信頼モデル、コンポーネント・インターフェース、証明書/CRL プロファイル、リポジトリ、証明書検証)に基づいて作業を実施した。 本手引では、それらの作業のどのフェーズでどのような観点に留意して「Asia PKI Interoperability Guideline」を参照したかを、認証局を建局するフローに合わせて解説している。

1.2 想定する読者

本手引きの読者として、認証局の設計者および運用者を想定する。

国際的な認証ドメイン間の信頼関係構築が具体的に想定されて、あるいは具体的には想定されなくても将来的な必要に備えて、「Asia PKI Interoperability Guideline」に準拠して認証局を建局するための情報を提供する。

また、既存認証局の運用者が「Asia PKI Interoperability Guideline」を使って自認証局が国際間接続の要件を満たしているのかどうかをチェックする場合の参考となる。

「Asia PKI Interoperability Guideline」は、国際間ビジネスシステムの設計者に対しても、自システムで PKI を利用するために必要な情報、特に国際間の認証ドメインの信頼関係構築と検証の要件についての情報を提供する。しかしながら、本手引では国際間ビジネスシステムの設計者については想定読者の範囲外とする。

1.3 応用可能な範囲

本手引きで述べるのは特恵 ECO パイロットシステムの事例であるが、特恵 ECO の

---

[1] “Asia PKI Interoperability Guideline” version1.0, Asia PKI Forum Interoperability Working Group, March, 2004

http://asia-pkiforum.org/Asia_PKI_Interoperability_Guidelinev1.0.pdf

http://www.japanpkiforum.jp/shiryou/APKI-F/APKI_IG_1_J.pdf (日本 PKI フォーラムによる日本語訳版)

システムに限定することなく、システムに PKI を利用する場合に考慮すべき点の情報として多くのビジネスに適用可能である。

2 ケーススタディ

この章では、平成 16 年度に日本とシンガポールの間で実施した、特恵原産地証明書を電子化するパイロットシステムへの「Asia PKI Interoperability Guideline」の適用事例を解説する。

以下、作業フェーズ毎に「Asia PKI Interoperability Guideline」の参照箇所とその際に留意すべき点を、補足情報を交えて記述する。表中の*斜体*の記述は、本パイロットシステムでの採用事項を示す。

2.1 認証局建局

2.1.1 準備作業

(1) 構成検討／プロダクト選定

<table>
<tr><td>1-1</td><td colspan="2">認証局の PKI コンポーネント構成を設計する。

本パイロットシステムでは下記とする。
・ 認証ドメイン内外からアクセスできるよう証明書パス構築と検証に必要な証明書と CRL/ARL を公開する LDAP サーバを設置する。</td></tr>
<tr><td rowspan="2"></td><td>1-1-1</td><td>留意点</td><td>他ドメインから参照できるリポジトリを構成要素とする。</td></tr>
<tr><td>参照</td><td>Part II technical Part / 2.1 PKI Components</td></tr>
<tr><td>1-2</td><td colspan="2">コンポーネント間インターフェースを設計する。

本パイロットシステムでは下記とする。
・ 他ドメインと Cross Certification を行う場合、PKCS#10 形式での証明書要求と、DER 形式による相互認証証明書の送付/受け取りを行う。
・ エンドエンティティ証明書は、エンドエンティティから CSR を受け取るのではなく、CA で鍵の生成を行って配布する。配布はエンドエンティティの秘密鍵(PKCS#8 形式)と証明書のチェーンからなる PKCS#12 形式とする。送付手段は、パイロットシステムであることを鑑み厳密な安全性確保を要件とせず電子メールでの送付とする。
・ VA 証明書については CSR を受け取り、それに対して発行した証明書を PKCS#7 形式で送付する。送付手段はエンドエンティティと同じく電子メールとする。</td></tr>
<tr><td rowspan="2"></td><td>1-2-1</td><td>留意点</td><td>他ドメインとの相互接続のための相互認証証明書要求フォーマットが PKCS#10、 相互認証証明書応答フォーマットが DER であること。</td></tr>
<tr><td>参照</td><td>Table.1 CA-CA Interface</td></tr>
<tr><td>1-3</td><td colspan="2">認証局のプロダクトを選定する。</td></tr>
</table>

	1-3-1	留意点	1-2-1 を実装したプロダクトを選定する。
		参照	(該当箇所なし)

(2) 環境設定

2-1	認証局内のハードウェアを設置する。OS 等の基本的なソフトウェアをインストール、設定する。		
	2-1-1	留意点	選定したプロダクトに合致する環境を構築する。プロダクト要件である。
		参照	(該当箇所なし)
2-2	PKI コンポーネントをインストール、設定する。		
	2-2-1	留意点	選定したプロダクトが正常に動作する環境を構築する。プロダクト要件である。
		参照	(該当箇所なし)
2-3	認証局内のコンポーネント間をネットワーク接続する。 *本パイロットシステムでは下記とする。* ・ *LDAP サーバへ CA からデータを LDAP で登録するため、認証局サーバマシンと LDAP サーバマシンの間で LDAPv3(ポート番号：既定値 389)の通信ができるよう設定する。*		
	2-3-1	留意点	認証局内に閉じた運用要件、プロダクト要件である。
		参照	(該当箇所なし)
2-4	外部ネットワークと接続する。		
	2-4-1	留意点	外部から LDAP サーバへの LDAPv3 のアクセスを提供すること。
		参照	Part II technical Part / 2.1 PKI Components

2.1.2 自己署名証明書の発行

(1) プロファイル設計

3-1	自己証明書のプロファイルを設計する。 ・ *本パイロットシステムの証明書プロファイルは「Appendix A」参照。*		
	3-1-1	留意点	authorityKeyIdentifier は任意だが、使用する場合は.keyID の設定が必須である。
		参照	Part II technical Part / 3.2.1 ROOT CA Certificate Profile
		補足	keyIdentifier の推奨される生成方法： 発行者の公開鍵のハッシュ値 (SHA1 160bit)。RFC3280 4.2.1.2 章に定義されている最初の計算方法。 (*1)各種証明書、証明書失効リスト、証明書発行要求に含まれる keyIdentifier は、証明書パス構築で証明書の識別に使われる。検証対象が認証ドメイン内に閉じている限りでは、keyIdentifier の生成方法は認証ドメイン内で統

			一がとれていれば問題ない。しかし異なる認証ドメイン間で信頼関係を構築する場合は問題となる。 発生する問題は以下の通り。 ・ keyIdentifier の生成方法が異なる PKI ドメイン間で相互認証証明書を発行すると、相互認証証明書を含む認証パスでは相互認証証明書の subjectKeyIdentifier と相互認証証明書の subjejct である認証局の発行する証明書の authorityKeyIdentifier 拡張の keyID が一致せず、keyIdentifier のチェーンは不整合を含むことになる。 この問題への対処法を下記に示す。 1. keyIdentifier 生成方法を認証ドメイン間でも統一するため RFC の推奨する方式を採用する。 2. 認証ドメイン間で相互認証を行う場合には要求元が CSR に subjectKeyIdentifier を記載し発行時はその値を証明書に記載することで発行側の keyIdentifier 生成方法を相互認証証明書に反映しないようにする。 ここで keyIdentifier 生成方法についての推奨を行っているのは対処 1 である。
	3-1-2	留意点	subjectKeyIdentifier は必須である。
		参照	Part II technical Part / 3.2.1 ROOT CA Certificate Profile
		補足	keyIdentifier の推奨される生成方法： 公開鍵のハッシュ値 (SHA1 160bit)。RFC3280 4.2.1.2 章に定義されている最初の計算方法。 (項目 3-1-1 補足(*1)参照)
	3-1-3	留意点	issuer、subject の文字コードに留意すること。 DN は UTF8STRING によってエンコードする。Country 属性のみは PrintableString によってエンコードする。
		参照	Part II technical Part / 3.5.1 Encoding rules of DirectoryName
	3-1-4	留意点	有効期限を要件に基づいて設定する。
		補足	自己署名証明書の有効期限は、CA の CP/CPS で決まるべきもの。CA が保証する暗号強度や、鍵更新のオペレーション、発行する証明書への影響など、考慮すべき点は多い。 *本パイロットシステムでは、実験開始から約 1 年間に渡り実験を行うという要求と、実験期間を大幅に越えての有効性を持つ証明書発行はできないことから、CA の自己署名証明書の有効期限を 2006 年 4 月 1 日とした。エンドエンティティ証明書の有効期限は CA の運用としてはやや異例だが、CA の自己署名証明書の有効期限とほぼ同じ 2006 年 3 月 31 日を設定する。*

(2) データ記載／発行

4-1	自己証明書に記載内容を入力し、発行する。		
	4-1-1	留意点	issuer、subject の文字コードに留意する。 DN はUTF8STRING によってエンコードする。Country 属性のみは PrintableString によってエンコードする。
		参照	Part II technical Part / 3.5.1 Encoding rules of DirectoryName

(3) リポジトリ格納

5-1	発行した自己署名証明書をリポジトリに格納する。		
	5-1-1	留意点	格納エントリの場所(DIT)の DN が、証明書に記述された subject の DN と一致すること。
		参照	Part II technical Part / 4.2 DIT
	5-1-2	留意点	CAエントリは下記いずれかのオブジェクトクラスでなければならない。 ・ pkiCA (2.5.6.22) ・ certificationAuthoritycertificationAuthority(2.5.6.16)
		参照	Part II technical Part / 4.3 Schema (objectclass, attribute) (1)CA
	5-1-3	留意点	自己署名証明書は属性 cACertificate (2.5.4.37)で格納しなければならない。
		参照	Part II technical Part / 4.3 Schema (objectclass, attribute) (1)CA

2.1.3 失効リストの発行

(1) プロファイル／配布ポリシ設計

6-1	失効リストのプロファイルと配布ポリシを設計する。 *本パイロットシステムでは下記の設計とする。* ・ *失効リストプロファイルは「Appendix A」参照。* ・ *単一 CRL(one complete CRL)と単一 ARL(one complete ARL)を発行する。この CA は下位 CA を持たず、他の CA との相互認証も行っていないので、現時点では ARL に格納される失効情報はない。今後、他の CA と相互認証を行うことがあればその失効情報を ARL に記載することになる。* ・ *LDAP サーバの CA エントリで公開する。*		
	6-1-1	留意点	失効リストの発行ポリシ(CRL を分割するか否か)を決定する。
		参照	Part II technical Part / 3.4.4 Value of cRLDistributionPoints and issuingDistributionPoints
		補足	CRL 発行ポリシは後述の iDP の設定内容や証明書の検証要件に影響する。

	6-1-2	留意点	issuingDistributionPoints の設定は失効リストの発行ポリシによって必須であるか否かが決まる。
		参照	Part II technical Part / 3.4.4 Value of cRLDistributionPoints and issuingDistributionPoints
		補足	*本パイロットシステムでは 必須項目である onlyConstrainsUserCerts 、 あるいは onlyConstrainsCACerts を設定する。さらに fullName.URI を設定する。ここにはエンドエンティティ証明書あるいは認証局の自己署名証明書の cRLDP.distPoint.fullname.URI と一致する値を設定する。前者の設定だけが置換攻撃に対する防御の要件であり、後者は必須ではないが、検証の便宜を図るため設定する。*
	6-1-3	留意点	authorityKeyIdentifier.keyID の計算方法に留意する。
		参照	Part II technical Part / 3.4.3 ARL/CRL Extensions
		補足	keyIdentifier の推奨される生成方法： 発行者の公開鍵のハッシュ値 (SHA1 160bit)。RFC3280 4.2.1.2 章に定義されている最初の計算方法。 (項目 3-1-1 補足(*1)参照)

(2) データ記載／発行

7-1	失効リストに記載内容を入力し、発行する。		
	7-1-1	留意点	issuer の文字コードを確認する。 DN は UTF8STRING によってエンコードする。Country 属性のみは PrintableString によってエンコードする。
		参照	Part II technical Part / 3.5.1 Encoding rules of DirectoryName
	7-1-2	留意点	issuingDistributionPoints.distPoint.fullName 内に特殊文字が含まれる場合、エスケープする。
		参照	Part II technical Part / 3.5.3 Escape method in the LDAPURL

(3) リポジトリ格納

8-1	発行した失効リストをリポジトリに格納する。		
	8-1-1	留意点	格納エントリの場所(DIT)を確認する。
		参照	Part II technical Part / 4.2 DIT
		補足	*本パイロットシステムでは CA エントリに格納するので失効リストに記述された issuer の DN が DIT の DN と一致すること。*
	8-1-2	留意点	オブジェクトクラスと属性を確認する。
		参照	Part II technical Part / 4.3 Schema (objectclass, attribute) (3)CRLDP

2.2　エンドエンティティへの証明書発行

2.2.1 準備作業

(1) 申請・配布方法の設計

9-1	エンドエンティティ証明書の使用者からの申請、発行後の使用者への送付方法を決定する。 ・ *本パイロットシステムでは、使用者からの申請ではなく認証局側で使用者の秘密鍵生成も行い PKCS#12 ファイルを電子メールで送付する。* ・ *検証局のみは PKCS#10 での申請、PKCS#7 の送付とする。*		
	9-1-1	留意点	認証ドメイン内で任意の方法を取ることができる。
		参照	Part II technical Part / 2.1 PKI Components

(2) プロファイル設計

ECO パイロットシステムで発行するエンドエンティティ証明書は以下の３種類である。

- ECO 署名用証明書
- S/MIME 用証明書（暗号化用、および署名用）
- VA 証明書

(a) 共通

10-1	エンドエンティティ証明書のプロファイルを設計する。 ・ *証明書プロファイルは「Appendix A」参照。*		
	10-1-1	留意点	authorityKeyIdentifier.keyID、subjectKeyIdentifier の計算方法に留意する。
		参照	Part II technical Part / 3.3.1 Common EE Profile
		補足	keyIdentifier の推奨される生成方法： 公開鍵のハッシュ値 (SHA1 160bit)。RFC3280 4.2.1.2 章に定義されている最初の計算方法。 (項目 3-1-1 補足(*1)参照)
	10-1-2	留意点	certificatePolicies の critical フラグの設定は、アプリケーション(たとえば Microsoft®Windows® 2000 またはそれ以前のバージョンのオペレーティング・システム)の実装を考慮して「non-critical」に設定することを推奨する。
		参照	Part II technical Part / 3.3.1 Common EE Profile
	10-1-3	留意点	cRLDistributionPoints は指定必須である。
		参照	Part II technical Part / 3.3.1 Common EE Profile
	10-1-4	留意点	basicConstraints は含まない。
		参照	Part II technical Part / 3.5.2 basicConstraints in EE certificate

(b) ECO 署名用証明書

11-1	ECO 署名用証明書のプロファイルを設計する。		
	11-1-1	留意点	keyUsage の値として digitalSignature をセットする。
		参照	Part II technical Part / 3.3.2 Identification Certificate (digital signature)
	11-1-2	留意点	有効期限を設計する。
		補足	*エンドエンティティ証明書は認証局の自己署名証明書の有効期限を越えない範囲とした。今回の ECO パイロットシステムでは、ECO 発行者は自分の証明書の有効期限を越えた ECO の有効期限を設定することはできない。証明書の有効期限を過ぎた時点で ECO の署名の有効性を保証することは、PKI の機能としてはできない。運用ルールでのカバー、あるいは電子情報の長期保存技術など、PKI 以外での保証が必要である。*

(c) S/MIME 用証明書（暗号化用、および署名用）

12-1	S/MIME 用証明書のプロファイルを設計する。 ・ *本パイロットシステムでは、S/MIME に使用する証明書を、暗号化用と署名用に分ける。*		
	12-1-1	留意点	keyUsage の値として digitalSignature(署名用ではこれのみ)、keyEncipherment(暗号化用ではこれのみ)をセットする。
		参照	Part II technical Part / 3.3.2 Identification Certificate (digital signature)
	12-1-2	留意点	subjectAltName.rfc822Name に電子メールアドレスを設定する。
		参照	Part II technical Part / 3.3.3 Secure E-Mail Certificate (data Encipherment and digital signature)

(d) VA 証明書

13-1	VA 証明書のプロファイルを設計する。		
	13-1-1	留意点	extKeyUsage に OCSPSigning(OID value: 1.3.6.1.5.5.7.3.9)を設定する。(optional)
		参照	Part II technical Part / 3.6 APPENDIX OCSP responder

2.2.2 エンドエンティティ証明書の発行

(1) データ記載／発行

14-1	エンドエンティティ証明書に記載内容を入力し、発行する。		
	14-1-1	留意点	issuer、subject の文字コードに留意する。 DN はUTF8STRING によってエンコードする。Country 属性のみは PrintableString によってエンコードする。
		参照	Part II technical Part / 3.5.1 Encoding rules of DirectoryName
	14-1-2	留意点	cRLDP 内に特殊文字が含まれる場合、エスケープする。
		参照	Part II technical Part / 3.5.3 Escape method in the LDAPURL

(2) リポジトリ格納（optional）

15-1	発行したエンドエンティティ証明書をリポジトリに格納する。 ・ *本パイロットシステムではエンドエンティティ証明書はリポジトリに格納しない。このため下記 15-1-1、15-1-2 は今回の作業では考慮する必要はない。*		
	15-1-1	留意点	格納エントリの場所（DIT）のDNが、証明書に記述されたsubjectのDNと一致すること。
		参照	Part II technical Part / 4.2 DIT
	15-1-2	留意点	オブジェクトクラスと属性を確認する。
		参照	Part II technical Part / 4.3 Schema (objectclass, attribute) (2)End Entity

(3) エンドエンティティへの送付

16-1	発行したエンドエンティティ証明書を使用者に送付する。 ・ *本パイロットシステムでは PKCS#12 ファイルを電子メールで送付する。*		
	16-1-1	留意点	認証ドメイン内で任意の方法を取ることができる。
		参照	Part II technical Part / 2.1 PKI Components

2.3　ドメイン間の信頼関係構築

2.3.1 信頼モデル選択

(1) 信頼モデル選択

<table>
<tr><td rowspan="3">17-1</td><td colspan="3">認証ドメイン間で構築する信頼モデルを選択する。

・ 本パイロットシステムでは CR モデルを採用する。</td></tr>
<tr><td>17-1-1</td><td>参照</td><td>Part II Technical Part/1.Trust Model</td></tr>
<tr><td></td><td>補足</td><td>本パイロットシステムの日本とシンガポールの間の信頼関係の要件は下記の通り。
・ 相手ドメインのエンドエンティティ(ECO 発行者等)の署名の検証のため、相手の証明書のパス構築、検証ができること。
・ ECO の送受信に使用する S/MIME が運用できること。
- 送信相手の暗号化用証明書が入手できること。
- 自分が付加した署名が受信者によって正しく検証できること。

「Asia PKI Interoperability Guideline」では代表的な信頼モデルとして Cross Certification(相互認証)と Cross Recognition(相互承認)を採用している。２つのモデルともに上記要件を満たす。その上で、関係構築の容易さでは Cross Recognition が勝る。
Cross Recognition の最大の課題は「証明書利用者はどうやって相手側の信頼点証明書を受け入れるか」であるが、この点は本パイロットシステムにおいては下記の理由から問題とはならない。
・ CA 間の相互承認関係構築のための CA 証明書交換は外交ルートを用いるなどで安全に行われることを想定できる。
・ 不特定多数の利用者が想定されるのではなく、ECO 送受信者や検証者が事前に確定されるシステムであることから、相手ドメインの CA 証明書をトラストアンカとしてそれらに配布することが比較的容易である。</td></tr>
</table>

2.3.2 相互承認

(1) 関係構築手順

18-1	トラストアンカとして自己署名証明書を相手ドメインに送付する。 ・ *本パイロットシステムでは、送付手段はパイロットシステムであることを鑑み厳密な安全性確保を要件とせず、電子メールでの送付とする。*		
	18-1-1	参照	Part II Technical Part/1.Trust Model/1.2 Cross Recognition(CR)
18-2	自ドメインの cerificatePolicy を相手ドメインに通知する。		
	18-2-1	参照	Part II Technical Part/1.Trust Model/1.2 Cross Recognition(CR)/fn.2
		補足	user_initial_policy_set として証明書パスの有効性検証に使われる情報である。

3 おわりに

「Asia PKI Interoperability Guideline」は、ECO パイロットシステムの基盤となる PKI 環境の構築作業全般に渡って有益な情報を提供している。これを活用することにより、今回のパイロットシステムのパートナーであるシンガポールとの PKI による信頼関係を円滑に構築することができた。

国際間で認証ドメイン間の信頼関係を構築し電子商取引の基盤とする際には、過去の実証実験によって認証ドメイン間接続の課題の洗い出しと解決策を提示している「Asia PKI Interoperability Guideline」の仕様に基づくことで、問題を回避して確実に PKI 環境を構築することができる。

PKI 環境構築にあたっては、ビジネスの特性により若干の要件の違いはあるにせよ、それ以上に共通する課題が多いことから、本手引の情報はさまざまなシステムに活用可能なものとなっている。

今後、本手引とともに「Asia PKI Interoperability Guideline」が広く活用され、PKI を基盤とした安全な電子商取引が発展することを期待する。